Building resilience:

The key to the continuity and long-term success of your business

The Bright Alternative

Explore: aztecgroup.co.uk | .eu | .us

AZTEC GROUP

Introduction

Before the disruption caused by the pandemic, it would be fair to say many people considered 'operational resilience' was just an extravagant term used to describe business continuity planning (BCP).

But while the two disciplines are closely related, their aims are very different. BCP focuses on eliminating single points of failure and on the recovery and restoration of service, whereas operational resilience is dedicated to engineering comprehensive service delivery that is resilient to disruption.

Those different objectives have been brought into sharper focus since COVID, which has seen operational resilience becoming a business priority. For many business leaders, including our own clients, it has become increasingly important that their companies and employees recognise the distinction between BCP and operational resilience, and appreciate the need for both.

Understandably, our clients want assurances that, whatever life throws at them, they can rely on us to help them weather any storms, and that their funds and fund operations can continue to function as normal.

What we'll cover in this guide:

Regulators step forward

Operational resilience found itself on the agenda for regulators in 2018, when consultation on a new regulation began, and the events of the last 18 months have ensured most organisations need little convincing that robust, regulated operational resilience is a must-have.

In March this year, the Bank of England (BoE), the UK Financial Conduct Authority (FCA), and the UK Prudential Regulation Authority (PRA) issued their Operational Resilience Policy Statements, which will come into force on 31 March 2022. Together, these statements set out a framework to promote the operational resilience of firms, and to ensure they invest in resilience to protect themselves, their consumers, and the financial system from disruption. In the European Union (EU) a similar approach is being adopted for financial services firms through its draft Digital Operational Resilience Act.

Operational Resilience Policy Statements:
Come into force
31 March 2022.

The impact on fund managers

The Operational Resilience Policy Statements apply to a range of financial services businesses including banks, building societies, designated investment firms, insurers, Recognised Investment Exchanges (RIEs), enhanced scope senior managers and certification regime (SM&CR) firms and entities authorised or registered under the Payment Services Regulations 2017 (PSRs 2017) or the Electronic Money Regulations 2011 (EMRs 2011).

The framework has been constructed based on the belief that firms must do the necessary work to identify their key services and set an impact tolerance for each – based on a maximum tolerable level of disruption to those services. So, instead of firms studying the resilience of individual systems, they are being encouraged more to consider the continuity of services that firms provide to their clients and other external users. Irrespective of whether your company is directly in scope, the framework still represents the current gold standard for operational resilience, and reflects the direction of travel for operational resilience, not only in the finance sector, but across all industry sectors globally.

We make this point because firms that are not adapting to this approach, at least in part, are placing themselves at a significant competitive disadvantage. Not only exposing themselves to the impacts of disruption, but also can expect to face increasing competition, rising client expectations, client retention challenges and the risk of failing to achieve regulatory compliance. It's therefore no surprise that several of our clients are already asking operational resilience questions that are framed by this policy in their supplier or service provider assessments.

What changes should investment firms expect?

UK regulation is built on the truism that "Disruption is inevitable", and it defines operational resilience as the ability of an organisation to prevent, adapt, respond to, recover and learn from operational disruptions. This effectively places operational resilience in the foreground of all investment decision-making, planning, service design, service delivery and operational activities.

From the perspective of an investment firm, you should already have professional risk management, incident management, service management and business continuity processes in place. While these all support your operational and financial resilience, the Operational Resilience Policy Statements mean you must also consider if you are able to continue to operate throughout a severe disruption, without intolerable harm to yourself, your clients, or to financial systems or markets. If you are in-scope of UK regulation you will need to prove this capability and evidence that you are taking reasonable measures – as well as making appropriate decisions and investments – to ensure you continue to be able to do so.

Where should firms start?

Whether firms are in-scope of operational resilience regulation or not, the following steps to assess your operational resilience capability should be considered as best practice.

1 Establish operational resilience within your corporate governance structures

Your firm's Board of Directors is responsible for the financial and operational resilience of your firm. It is also accountable to regulators and clients for any harm caused due to disruption in the service you offer. Therefore, it is essential that your Board is accountable for identifying your firm's important business services, as well as setting the impact tolerances described below. The Board must also prioritise any investment or cultural changes that may be required to improve operational resilience.

2 Know your services

Identify each service you offer or perform, and determine which are the most important. This determination should be based on which services, if disrupted, would pose a significant risk to your firm's safety and soundness, or where disruption could cause intolerable harm to your clients – or to financial systems and markets – from which they could not easily recover. The FCA defines intolerable harm as much more severe than inconvenience or harm. For both 'harm' and 'inconvenience' it would expect firms to be able to remediate any disruption so that no ill effects would be felt in the medium or long-term by clients or markets.

Firms should map all the resources and components needed to perform each service, including facilities, people, teams, equipment and infrastructure, IT applications, and internal and external service providers. You should consider the impact to the overall service if any one of these resources or components were removed or severely disrupted. When mapping services, try to cross-reference resources and components common to many services. This mapping will help to identify vulnerabilities in your operations, and possibly help to address them. When addressing vulnerabilities it's essential not only to consider the importance of the services for which a vulnerability exists but also to consider whether a single vulnerability exists for many services.

By knowing what's important, what's vulnerable and where disruption could cause the most harm or have the most widespread effect, you can determine investment priorities and drive strategic and tactical decision-making.

3 Set realistic impact tolerances for each service

An impact tolerance is the maximum level of impact that can be tolerated before your firm's safety or soundness are at risk, or you risk intolerable harm to your clients, or significant lasting damage to financial systems or markets. The impact tolerance should specify that a particular important business service should not be disrupted beyond a certain period of or point in time, as well as consider any other relevant metrics, such as cost, regulatory breach, or client or service volumes. Impact tolerances should also consider peak times or periods of increased activity where impact may become evident faster.

Impact tolerances differ from risk appetite, as risk appetite considers both impact and likelihood, and mitigation often focuses on addressing the cause or reducing the likelihood. However, the cause or likelihood of a disruption plays no part in assessing the impact tolerance, as "disruption is inevitable". Therefore, in most cases, due to the removal of likelihood, your impact tolerance will exceed your risk appetite.

Both risk appetite and impact tolerance are essential in supporting your firm's operational and financial resilience, but aligning impact tolerances to important business services will give you a better indication of where investments need to be made. It will also help to determine which vulnerabilities need to be addressed to ensure you continue to deliver within your impact tolerances despite – and throughout – a severe disruption.

What next?

After you have identified and mapped your firm's important business services, and set your impact tolerances, several steps can be taken to ensure you remain within these impact tolerances throughout any severe disruption.

If you are in-scope of the UK regulation, you will need to demonstrate you are able to remain within your impact tolerances by no later than 31 March 2025.

Even for firms out-of-scope of the regulation, best practice is to carry out the following activities regularly:

Regularly review important business services and reassess the resources required, to help uncover any vulnerabilities.

Incorporate operational resilience assessments into service design and service introduction processes. If you can calculate the future importance of a service and identify vulnerabilities before service deployment, you can address them before the service goes live, possibly avoiding unnecessary costs or risk.

Regularly review your impact tolerances. These can change as services evolve, as your own business needs and priorities change (as well as those of your clients), or due to changes in regulation or the financial markets.

Regularly assess your external service providers. As well as asking questions about the specific services they provide, ask about their operational resilience position and capability. It is never good when someone else's business disruption becomes your disruption.

Test your firm's ability to stay within impact tolerance by using scenario tests. This approach will be familiar to your firm's BCP practitioners, and as well as proving capability, it is also crucial in identifying vulnerabilities previously not considered.

After any test, or as soon as possible after a real disruption, conduct a 'lessons learnt' exercise. It is vital to determine whether you can successfully adapt and respond, or even to prevent similar disruption in future.

Improving your firm's operational resilience

1

Ensure that all your operational processes are documented. Where possible use workflows or checklists to ensure that activities are repeatable and consistent.

2

Ensure that all staff are up to date with training requirements and avoid the consolidation of knowledge in small numbers of staff. Periods of cross-training or rotation of work allocations can provide many resilience and productivity benefits, as well as potential staff development opportunities.

3

Consider alternative procedures for essential activities. For example, could a current activity performed by an IT application also be performed manually? Could an essential resource or service be sourced from elsewhere? Could work be performed by other staff if personnel are impacted?

4

Where possible, document what would be required and how to perform any alternative procedures. Make new procedures part of the functional training for the activity, and where possible, test it regularly. The alternate procedure may not be efficient or practical over time, but it may enable you to stay within impact tolerance until the cause of disruption is resolved and service restored.

5

Where possible, and while following your firm's physical and IT security policies, encourage staff to always take mobile devices required for their work, such as laptops and mobiles, home with them. Disruptions often occur outside of office hours. Should you be deprived of an office location overnight, your work-from-home capabilities could be severely compromised if large numbers of staff leave their devices in the office.

6

Know your suppliers and service providers and talk to them about their operational resilience capability.

Final thoughts…

Given that operational resilience has become such a key topic for the industry, it's no surprise that the regulatory burden has increased, and that firms must be seen to be doing more to demonstrate their own preparations.

But good operational resilience practice is not just about avoiding business risks. It also actively promotes business flexibility and agility, enabling an organisation to better respond to client requirements, business and organisational challenges, and supporting growth and efficiency. In other words, operational resilience is not just about preventing the worst outcomes from happening, it's about creating an environment where true operational excellence can be achieved.

Get in touch

If you would like to discuss your firm's operational resilience, as well as how Aztec can support you, please talk to either your usual Aztec Group contact or get in touch with:

Paul Alcock
Senior Business Continuity Manager
Telephone: +44 (0) 238 235 5772
Email: Paul.Alcock@aztecgroup.co.uk

Emily Sturgess
Head of Operational Resilience
Telephone: +44 (0) 1534 833045
Email: Emily.Sturgess@aztecgroup.co.uk

The Bright Alternative

Explore: aztecgroup.co.uk | .eu | .us

Private Equity Fund Services
Real Asset Fund Services
Private Debt Fund Services
Corporate Services

AZTEC
GROUP